



POLÍTICA DE CONTROL DE ACCESO LÓGICO

Junta Nacional de Jardines Infantiles
2021

TABLA DE CONTENIDO

1. OBJETIVO	3
2. ALCANCE	3
3. ROLES Y RESPONSABILIDADES	3
3.1. Sección de Tecnologías de Información	3
3.2. Funcionarios de JUNJI	4
3.3. Jefaturas de Área	4
3.4. Unidad de Seguimiento, Gestión y Mejora Continua de Gestión del Departamento de Gestión y Desarrollo de Personas	4
4. DEFINICIONES DE LA POLITICA	4
4.1. Control de Acceso	4
4.2. Servicios de Red	5
4.3. Administración de las Cuentas de Usuarios	5
4.4. Las Cuentas de Usuarios son Individuales	6
4.5. Protección de Estaciones de Trabajo	6
4.6. Cambio periódico de las Contraseñas	6
4.7. Asignación de Contraseñas Expiradas y Reasignación de Contraseñas	7
4.8. Límite a Intentos Fallidos de Ingreso	7
4.9. Recordatorios de Contraseñas	7
4.10. Registro y Monitoreo	7
4.11. Cuentas de administrador y accesos privilegiados	8
4.12. Gestión y uso de contraseñas	8
4.13. Baja de cuentas de usuarios	9
5. PERIODICIDAD DE EVALUACIÓN Y REVISION	9
6. DIFUSIÓN	9
7. CONTROL DEL DOCUMENTO	10



POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO JUNTA NACIONAL DE JARDINES INFANTILES

1. OBJETIVO

El presente documento establece los lineamientos para restringir el acceso a los sistemas informáticos y a los activos de información disponibles en la red, de manera que los usuarios autenticados accedan exclusivamente a los recursos sobre los cuales tengan derecho y/o permisos.

2. ALCANCE

El sistema de gestión de la información abarca todos los recursos computacionales que requieran la creación de cuentas de acceso y den soporte a los productos estratégicos de la institución. Incluye todos los usuarios, operadores y administradores.

La presente política es aplicable a la gestión de funcionarios de planta, contrata y el personal que se desempeñe en la calidad de honorarios y que formen parte de la JUNJI, y en general a cualquier otra persona o empresa que preste servicios y que se encuentre contratado por la institución.

Los controles de la normativa NCh-ISO 27001:2013 que aborda esta política de seguridad son:

- A.9.1.1 Política control de acceso.
- A.9.1.2 Acceso a las Redes y a los Servicios de Red.
- A.9.2.3 Gestión de acceso privilegiado.
- A.9.4.2 Procedimiento de inicio de sesión seguro.
- A.9.4.3 Sistema de gestión de contraseñas.

3. ROLES Y RESPONSABILIDADES

3.1. Sección de Tecnologías de Información:

- Crear las cuentas de usuario y velar por el almacenamiento y actualización de la información, así como también de la baja de cuentas cuando corresponda.
- Administrar el control de acceso a los sistemas de información y a los recursos de la red institucional.
- Registrar los accesos exitosos e intentos fallidos a los sistemas de información.
- Administrar los privilegios de acceso a los sistemas de información y recursos de red.
- Gestionar las solicitudes de acceso a los recursos desde las distintas áreas de la institución.
- Disponer sistemas de control de acceso que provean una gestión segura de las contraseñas.



POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO JUNTA NACIONAL DE JARDINES INFANTILES

3.2. Funcionarios de JUNJI

- Todo funcionario de JUNJI tendrá la obligación de informar al Encargado de Seguridad de la Información cualquier actividad que contravenga lo aquí estipulado o que simplemente le resulte sospechosa.
- Cumplir las reglas de esta política para el manejo de sus cuentas de usuario y contraseñas.

3.3. Jefaturas de Área

- Solicitar la creación de cuentas de usuarios; agregar o quitar recursos de red de usuarios (accesos a sistemas, roles, permisos de navegación, etc.); recursos técnicos (computador, notebook, teléfonos IP o celulares, etc.); y baja de cuentas de usuarios utilizando los canales para estos efectos y lo indicado en procedimientos de: “Asignación de Acceso de Usuarios”, “Eliminación o ajuste de los derechos de accesos” y “Inicio de sesión seguro”.

3.4. Unidad de Seguimiento, Gestión y Mejora Continua de Gestión del Departamento de Gestión y Desarrollo de Personas

- Generar e informar por medio de un listado o informe de carácter trimestral sobre los usuarios que a nivel nacional (unidades educativas y oficinas) fueron desvinculados o cesaron funciones en la institución en el periodo antes mencionado.

4. DEFINICIONES DE LA POLITICA

4.1. Control de Acceso

- Para todo sistema de información de la institución, el usuario deberá poseer una cuenta personal que lo identifique. La identificación se realizará normalmente por un Username, Usuario o “Código de Usuario” junto con una contraseña.
- Habrán implantados controles de acceso lógico (lectura, escritura, eliminación y ejecución) que aseguren los niveles de acceso requeridos por el sistema, para asegurar que la funcionalidad de la aplicación se corresponde con la funcionalidad del trabajo.
- Tanto los controles de acceso como las protecciones contra acceso no autorizado permitirán mantener un registro de los eventos de importancia que involucran el uso y la administración de identidades de usuario e información de autenticación.



POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO JUNTA NACIONAL DE JARDINES INFANTILES

- Deberán existir controles para garantizar la salida segura de la información sensible hacia otras aplicaciones, terminales, monitores o cualquier otro dispositivo de salida. Estos controles tendrán en cuenta la ubicación física de los dispositivos que manejen la salida de la información sensible.

4.2. Servicios de Red

A continuación, se enumeran los principios de seguridad en red, los cuales pretenden prevenir el acceso no autorizado a los servicios de red; ellos están soportados en detalle por los estándares correspondientes.

- Sólo se dará acceso a los usuarios a los servicios que han sido autorizados a utilizar.
- Existirán mecanismos de autenticación adecuados para cualquier acceso remoto a través de un canal seguro habilitado para tal efecto (VPN).
- Existirá una segregación de red adecuada, de forma que se protejan los servicios y sistemas de red.
- Se forzará el cumplimiento de los principios de la política de controles de acceso a través de redes compartidas, tomando en cuenta los controles de acceso a los servicios de red adecuados que aseguren el cumplimiento de las necesidades de la Institución.
- Se analizarán los riesgos asociados a la implementación de mecanismos automáticos de identificación de dispositivos, acceso remoto a puertos de diagnóstico, configuración, y controles de enrutamiento.
- Habrá mecanismos implantados para asegurar un acceso autorizado y controlado a cualquier punto de acceso inalámbrico.

4.3. Administración de las Cuentas de Usuarios

- Para todo usuario nuevo que se cree como cuenta, esta función recaerá y será realizado por la Sección de Tecnologías de la Información.
- Para cuentas de acceso a servicios de red:
 - ✓ La creación de un nuevo Usuario debe ser solicitado por el **jefe de la Unidad** correspondiente a través de los formularios destinados para dicho efecto con la debida autorización de las jefaturas de área solicitante.
 - ✓ La **Sección TI** creará la cuenta y será responsable de velar por el almacenamiento y actualización de tal información.

POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO JUNTA NACIONAL DE JARDINES INFANTILES

- ✓ La nomenclatura utilizada para la composición del usuario que identifica cada cuenta y que señala las porciones de nombres y apellidos, así como largo mínimo de tal identificador. En caso de existir coincidencia se agregan las primeras letras del segundo nombre o la primera letra del segundo apellido.
- Para cuentas de acceso a sistemas de información de la institución:
 - ✓ La creación de un nuevo usuario debe ser gestionado por el **jefe de la Unidad** correspondiente mediante los formularios destinados para dicho efecto.
 - ✓ **La Sección TI** asignará los privilegios a la nueva cuenta de acuerdo con las funciones a realizar.
 - ✓ La nomenclatura utilizada para la composición del Usuario dependerá de la funcionalidad de ingreso de cada sistema.
- Cualquier solicitud de cambio de privilegios asignados a una cuenta debe ser validada por **el jefe de la Unidad** de dependencia directa del funcionario mediante los formularios destinados para dicho efecto.
- En caso de cambio de unidad del usuario, se debe además validar la eliminación de permisos o accesos a sistemas y aplicaciones por parte de la unidad a la que deja de pertenecer, y del mismo modo la jefatura a donde llega debe solicitar permisos a sistemas o aplicaciones si es necesario en su nueva función. Para ambos casos existen formularios de solicitud de permisos.

4.4. Las Cuentas de Usuarios son Individuales

- El usuario y la contraseña asociados a una cuenta de son únicas e individuales, estando prohibido facilitarlos a un tercero.
- Esta política rige tanto para usuarios finales (internos o externos), operadores, administradores y auditores.
- El usuario dueño de la cuenta es responsable de las actividades que se efectúen con su cuenta.
- Está prohibido el uso de un nombre de usuario ajeno.

4.5. Protección de Estaciones de Trabajo

- Todas las estaciones de trabajo deben tener una contraseña de ingreso y un protector de pantalla (screensaver) con contraseña y activación máxima de 5 minutos.

4.6. Cambio periódico de las Contraseñas



POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO JUNTA NACIONAL DE JARDINES INFANTILES

- Todos los usuarios deben cambiar su contraseña cada 90 días.
- Las contraseñas no deben ser reutilizadas en el tiempo ni en distintos sistemas. Los usuarios no deben construir contraseñas que sean idénticas o similares a las últimas ya utilizadas, de acuerdo con el valor definido como estándar de la institución para cantidad de contraseñas históricas a chequear.

4.7. Asignación de Contraseñas Expiradas y Reasignación de Contraseñas

- La contraseña asignada a una nueva cuenta obligará al usuario a cambiarla durante su primera conexión.
- La solicitud de cambio de contraseña por olvido se debe efectuarse a la **Sección de TI**, previa identificación positiva del usuario que lo solicita.
- Toda reasignación de contraseñas será registrada en la bitácora del sistema y deberá notificarse al usuario de la cuenta, a su casilla de correo registrada al crear la cuenta asociada. Esto permite detectar suplantación de identidad.
- **La Sección de TI** dispondrá de herramientas que eviten posibles tácticas de suplantación de identidad de usuarios u otros artilugios para obtener información a la cual no tiene acceso normalmente (lo que en el campo de la seguridad informática se denomina ingeniería social).

4.8. Límite a Intentos Fallidos de Ingreso

- Para prevenir ingresos mediante la prueba de varias posibles contraseñas, se limita la aceptación de intentos consecutivos de ingreso, configurado como estándar de la institución. Después de los intentos fallidos, la cuenta de usuario será deshabilitada. El usuario notificará a la mesa de ayuda de la **Sección de TI**, quien habilitará la cuenta, previa verificación de la identidad del usuario y generando el informe de atención respectivo.
- En caso de usuarios externos sólo podrá ser reactivado el acceso por consentimiento del contacto establecido al momento de crear la cuenta del usuario.

4.9. Recordatorios de Contraseñas

- Queda absolutamente prohibido anotar las contraseñas de acceso en lugares públicos.

4.10. Registro y Monitoreo

- Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad.



4.11. Cuentas de administrador y accesos privilegiados

- La cuenta de usuario administrador de un sistema de información corresponde a la cuenta de usuario que permite al **Administrador del Sistema** realizar tareas específicas de usuario a nivel directivo, como, por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema. Estas cuentas deben ser administradas por la **Sección de TI**, y sus actividades deben ser registradas en logs que se mantendrán protegidos para actividades de auditoría y análisis forense.
- El funcionario que por las responsabilidades propias de su cargo tiene una necesidad legítima de usar los privilegios de administración, debe tener su propia cuenta administrativa que se utilizará para llevar a cabo dichas funciones. El uso de la cuenta de administrador de un sistema de información debe restringirse a un grupo limitado de usuarios y a situaciones de emergencia. Esto protegerá a la cuenta de administrador principal y proporcionando una pista de auditoría de las actividades administrativas.
- Los derechos de acceso privilegiado se asignarán a través de una cuenta de usuario distinta a las cuentas asignadas a las actividades institucionales regulares. Las actividades regulares no se realizarán desde una cuenta de usuario privilegiada.
- El otorgamiento de accesos a los sistemas de información con mayores privilegios (por ejemplo, acceso a: bases de datos, código fuente, etc.) a funcionarios/as que no pertenezcan a la Sección de TI, debe ser solicitado por la Jefatura correspondiente o quién delegue, autorizados por el propietario del activo y por el Encargado/a de Seguridad de la Información.

4.12. Gestión y uso de contraseñas.

- La contraseña corresponde a la información secreta de autenticación de toda cuenta de usuario, y la asignación de estas deben ser administrada por la **Sección de TI**.
- La **Sección de TI** dispondrá de uno o más sistemas de autenticación que permitan cumplir los siguientes requerimientos:
 - ✓ Cada cuenta de usuario y su contraseña es individual.
 - ✓ Las contraseñas deben ser de una composición fuerte estableciendo un largo mínimo y ser alfanuméricas, es decir, letras, números y opcionalmente algún signo especial.
 - ✓ Solicitar cambios periódicos de las contraseñas.
 - ✓ Prevenir ingresos mediante la prueba de varias posibles contraseñas, limitando la aceptación de intentos consecutivos de ingreso.



POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO JUNTA NACIONAL DE JARDINES INFANTILES

- ✓ Registrar los intentos logrados y los fallidos.
- ✓ La contraseña asignada a una nueva cuenta obligará al usuario a cambiarla durante su primera conexión.
- ✓ No mostrar contraseñas en la pantalla mientras se ingresan.
- ✓ No transmitir contraseñas en texto sin cifrar a través de una red;
- ✓ Restringir el acceso a los datos de autenticación con controles de acceso y encriptación para evitar que personas no autorizadas logren obtención de los datos.

4.13. Baja de cuentas de usuarios.

- La Unidad de Seguimiento, Gestión y Mejora Continua de Gestión del Departamento de Gestión y Desarrollo de Personas (GESDEP), tendrán como función informar y hacer llegar trimestralmente a la Unidad Continuidad Operativa de TI un listado con el detalle de los funcionarios cesados o desvinculados en la Institución (Oficinas y Unidades Educativas) en dicho periodo. Con esta información se realizará el bloqueo de las cuentas y/o su eliminación de los distintos sistemas a los que tenían acceso los funcionarios cesados.
- Por su parte los Jefes de Unidades deberán informar a TI (Unidad Continuidad Operativa o mesa de ayuda) cuando un funcionario sea desvinculado o renuncie, con el fin de bloquear y/o eliminar los accesos que dicho usuario haya tenido sobre sistemas o plataformas institucionales. De esta manera se busca resguardar la confidencialidad, disponibilidad e integridad de los datos y evitar accesos a información no autorizados y de complementar lo indicado en el punto 4.3 y 4.4 de la presente política.

5. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN

El presente documento será revisado cada dos años, o cuando la institución lo requiera, de manera de asegurar la continuidad e idoneidad del control, considerando los cambios que puedan producirse, tales como: enfoques a la gestión de seguridad de la información, cambios legales, normativos o estatutarios, cambios tecnológicos, recomendaciones frente a amenazas y vulnerabilidades, instrucciones que emanen de autoridades pertinentes, circunstancias de la Institución, entre otras.

6. DIFUSIÓN

La presente política deberá difundirse a todas y todos los funcionarios del Servicio a través del Correo Electrónico Institucional y/o publicado en la Intranet Institucional.



POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO
JUNTA NACIONAL DE JARDINES INFANTILES

7. CONTROL DEL DOCUMENTO

HISTORIA DEL DOCUMENTO	
Nombre del Documento:	Política de Control de Acceso Lógico
Creado por:	Jefes de Departamento y/o Secciones
Responsable del Documento:	Encargada de Seguridad de la Información
Fecha de Creación:	18/06/2019

CONTROL DE VERSIONES			
Versión	Fecha de Modificación	Motivo	Páginas / secciones modificadas
1.0	18-06-2019	Creación del documento	Todas
1.1	09-07-2019	Aprobación	Todas
1.2	17-07-2020	Redacción (R) e Incorporación (I)	R: puntos 4.3 - 4.5 I: puntos 3.4 - 4.13
1.3	01-09-2021	Actualización	Alcance (controles ISO), Firmas

FIRMAS	
 <small>Chr (Oct 29, 2021 18:46 ADT)</small> Claudio Henriquez Rebolledo Encargado de Unidad Continuidad Operativa TI	 <small>Lorena Osorio Díaz (Oct 29, 2021 08:24 ADT)</small> Lorena Osorio Díaz Directora Departamento de Gestión y Desarrollo de Personas
 <small>Marco Ibacache O. (Oct 31, 2021 16:34 ADT)</small> Marco Ibacache Olguín Encargado de Sección de Tecnologías de Información Encargado de Seguridad de la Información	



POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO LÓGICO
JUNTA NACIONAL DE JARDINES INFANTILES

Comité de Seguridad de la Información		
Nombre del Profesional	Departamento o Unidad	Revisión y Aprobación
Cristian Cerda Pérez	Comunicaciones y Ciudadanía	 <u>Cristian Cerda (Oct 28, 2021 12:18 ADT)</u>
Enzo Marzán Oyarzún	Recursos Financieros	 <u>Enzo Marzán Oyarzún (Oct 27, 2021 13:13 ADT)</u>
Javiera Osorio Estrada	Gestión y Desarrollo de Personas	 <u>Javiera Osorio Estrada (Oct 25, 2021 16:27 ADT)</u>
Julio Saavedra Rojas	Fiscalía y Asesoría Jurídica	
Constanza Sabater Orellana	Calidad Educativa	
Patricio Reyes Martínez	Tecnologías de la Información	 <u>Patricio Reyes (Oct 25, 2021 10:09 ADT)</u>



JUNJI_A.9_Política Control de Acceso Lógico_V1.3

Final Audit Report

2021-10-31

Created:	2021-10-25
By:	Patricio Reyes (PREYES@JUNJI.CL)
Status:	Signed
Transaction ID:	CBJCHBCAABAAph6vE1Hv7XQjUSToLB45VQRoB5ewR-pn

"JUNJI_A.9_Política Control de Acceso Lógico_V1.3" History

-  Document created by Patricio Reyes (PREYES@JUNJI.CL)
2021-10-25 - 1:05:38 PM GMT- IP address: 190.22.9.160
-  Document e-signed by Patricio Reyes (PREYES@JUNJI.CL)
Signature Date: 2021-10-25 - 1:09:39 PM GMT - Time Source: server- IP address: 190.22.9.160
-  Document emailed to Javiera Osorio Estrada (jfosorio@junji.cl) for signature
2021-10-25 - 1:09:41 PM GMT
-  Email viewed by Javiera Osorio Estrada (jfosorio@junji.cl)
2021-10-25 - 7:26:37 PM GMT- IP address: 200.74.110.37
-  Document e-signed by Javiera Osorio Estrada (jfosorio@junji.cl)
Signature Date: 2021-10-25 - 7:27:19 PM GMT - Time Source: server- IP address: 200.74.110.37
-  Document emailed to Julio Saavedra Rojas (jasaavedra@junji.cl) for signature
2021-10-25 - 7:27:22 PM GMT
-  Email viewed by Julio Saavedra Rojas (jasaavedra@junji.cl)
2021-10-26 - 4:18:33 PM GMT- IP address: 186.11.84.173
-  Document e-signed by Julio Saavedra Rojas (jasaavedra@junji.cl)
Signature Date: 2021-10-26 - 4:20:32 PM GMT - Time Source: server- IP address: 186.11.84.173
-  Document emailed to Enzo Marzán Oyarzún (emarzan@junji.cl) for signature
2021-10-26 - 4:20:34 PM GMT
-  Email viewed by Enzo Marzán Oyarzún (emarzan@junji.cl)
2021-10-26 - 7:09:29 PM GMT- IP address: 201.239.120.72

 Email viewed by Enzo Marzán Oyarzún (emarzan@junji.cl)

2021-10-27 - 12:41:21 PM GMT- IP address: 200.111.176.225

 Document e-signed by Enzo Marzán Oyarzún (emarzan@junji.cl)

Signature Date: 2021-10-27 - 4:13:59 PM GMT - Time Source: server- IP address: 200.111.176.225

 Document emailed to Constanza Sabater (csabater@junji.cl) for signature

2021-10-27 - 4:14:03 PM GMT

 Email viewed by Constanza Sabater (csabater@junji.cl)

2021-10-27 - 7:38:09 PM GMT- IP address: 186.78.90.157

 Document e-signed by Constanza Sabater (csabater@junji.cl)

Signature Date: 2021-10-27 - 7:40:54 PM GMT - Time Source: server- IP address: 186.78.90.157

 Document emailed to Cristian Cerda (ccerda@junji.cl) for signature

2021-10-27 - 7:40:57 PM GMT

 Email viewed by Cristian Cerda (ccerda@junji.cl)

2021-10-28 - 3:18:20 PM GMT- IP address: 190.151.104.210

 Document e-signed by Cristian Cerda (ccerda@junji.cl)

Signature Date: 2021-10-28 - 3:18:45 PM GMT - Time Source: server- IP address: 190.151.104.210

 Document emailed to Chr (cahenriquez@junji.cl) for signature

2021-10-28 - 3:18:47 PM GMT

 Email viewed by Chr (cahenriquez@junji.cl)

2021-10-28 - 9:46:00 PM GMT- IP address: 186.20.243.215

 Document e-signed by Chr (cahenriquez@junji.cl)

Signature Date: 2021-10-28 - 9:46:34 PM GMT - Time Source: server- IP address: 186.20.243.215

 Document emailed to Lorena Osorio Díaz (liosorio@junji.cl) for signature

2021-10-28 - 9:46:36 PM GMT

 Email viewed by Lorena Osorio Díaz (liosorio@junji.cl)

2021-10-29 - 11:23:41 AM GMT- IP address: 190.151.20.194

 Document e-signed by Lorena Osorio Díaz (liosorio@junji.cl)

Signature Date: 2021-10-29 - 11:24:21 AM GMT - Time Source: server- IP address: 190.151.104.210

 Document emailed to Marco Ibacache O. (mibacache@junji.cl) for signature

2021-10-29 - 11:24:23 AM GMT

 Email viewed by Marco Ibacache O. (mibacache@junji.cl)

2021-10-31 - 7:33:38 PM GMT- IP address: 190.93.239.109



Adobe Sign



Document e-signed by Marco Ibacache O. (mibacache@junji.cl)

Signature Date: 2021-10-31 - 7:34:18 PM GMT - Time Source: server- IP address: 190.93.239.109



Agreement completed.

2021-10-31 - 7:34:18 PM GMT



Adobe Sign